UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/435,899	11/08/1999	PAUL JOSEPH SEGER	TU999050	5856

7590 10/23/2003

ROBERT M SULLIVAN
IBM CORPORATION
INTELLECTUAL PROPEERTY LAW
9000 S RITA ROAD 90A/9032
TUCSON, AZ 85744

EXAMINER	
BETIT, JACOB F	

ART UNIT	PAPER NUMBER
2175	4

DATE MAILED: 10/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application N .	Applicant(s)	
	09/435,899	SEGER, PAUL JOSEPH	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this c mmunication appears on the cover sheet with the correspondence address --

Peri d f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-50 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-50 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2 and 3 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Specification

1. The arrangement of the disclosed application does not conform with 37 CFR 1.77(b).

The title is underlined in the discolosed specification. The title should not be underlined and/or **boldfaced**. Appropriate corrections are required according to the guidelines provided below:

2. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(e) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(f) BRIEF SUMMARY OF THE INVENTION.
(g) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).

(h) DETAILED DESCRIPTION OF THE INVENTION.
(i) CLAIM OR CLAIMS (commencing on a separate sheet).
(j) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(k) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

3. The abstract of the disclosure is objected to because it exceeds 150 words. Correction is required. See MPEP § 608.01(b).

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-50 rejected under 35 U.S.C. 103(a) as being unpatentable over Schneck et al. (U.S. patent No. 5,933,498) in view of Davis (U.S. patent No. 4,941,201).

As to claim 1, Schneck et al. teaches the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 23, line 56 through column 24, line 4, where the "user table" is read on the permission list that has a list of users or groups of users and there qualities and quantities of access), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; the processor receiving the user authentication messages from the data storage drive , combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity, and the user authorization or denial to the data storage drive (see column 10, line 59 through column 11, line 3).

Schneck et al. does not teach a portable security system for managing access to a portable data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, the portable security system comprising: a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in said data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the

wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface; and transmitting via the wireless interface.

Davis teaches a portable security system (see column 3, lines 32-38, where a security system on the data device is described) for managing access to a portable data storage cartridge (see column 2, line 45), the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive (see column 3, lines 24-29) when mounted in the data storage drive (see column 5, lines 55-61, where "mounted in the data storage drive" is read on "brought into proximity"), the portable security system comprising: a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in said data storage drive (see column 3, lines 19-23); and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface (see column 6, lines 22-59); the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface (see column 3, lines 19-23); the computer processor receiving via the wireless interface; and transmitting via the wireless interface (see column 3, lines 19-23).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. to include a portable security system for managing access to a portable data storage cartridge, the data

storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, the portable security system comprising: a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in said data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface; and transmitting via the wireless interface.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. by the teachings of Davis because a portable security system for managing access to a portable data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, the portable security system comprising: a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in said data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface; and transmitting via the wireless interface

would be one form of a storage device that could tangibly embody a package of digital data comprising protected portions (see Schneck et al., column 7, lines 28-30).

As to claims 2 and 16, Schneck et al. as modified, teaches wherein the wireless interface comprises an RF interface (see Davis, column 5, lines 55-61 and see column 21, lines 31-33, where 100 kHz is in the RF range or the Electromagnetic Spectrum).

As to claims 3, 17, 30, and 41, Schneck et al. as modified, teaches wherein each the user identifier comprises a user symbol and a user decrypting key (see Schneck et al., table I), wherein the user authentication message comprises an encrypted user authentication message which may be decrypted by the user decrypting key, and wherein the computer processor conducts the combination by decrypting the user authentication message by the user decrypting key (see Schneck et al., column 10, line 59 through column 11, line 3).

As to claims 4, 18, 31, and 42, Schneck et al. as modified, teaches wherein the user decrypting key comprises a sender public key, and wherein the predetermined algorithm comprises a public key cryptographic algorithm (see Schneck et al., column 10, line 59 through column 11, line 3).

As to claims 5, and 19, Schneck et al. as modified, teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key,

and wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, whereby the user authentication message is known to have come from the user (see Schneck et al., column 10, line 59 through column 11, line 3).

As to claims 6, 20, and 44, Schneck et al. as modified, teaches wherein the computer processor user table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to the user table (see Schneck et al., column 23, lines 6-55 and see column 32, lines 15-27).

As to claims 7, 21, and 45, Schneck et al. as modified, teaches wherein the computer processor user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct (see Schneck et al., column 23, line 56 through column 24, line 4).

As to claims 8, 22, and 46, Schneck et al. as modified, teaches wherein the computer processor user table comprises a separate entry for each the user identifier,

the entry comprising all the permitted activities the user is authorized to conduct (see Schneck et al., column 23, line 56 through column 24, line 4).

As to claims 9 and 23, Schneck et al. as modified, teaches wherein the computer processor additionally comprises a nonvolatile memory storing the user table (see Schneck et al., column 14, line 66 through column 15, line 13).

As to claims 10, 24, 36, and 47, Schneck et al. as modified, teaches wherein the computer processor additionally comprises a class table comprising at least a unique class identifier for each authorized class of users and at least one permitted activity the class of users is authorized to conduct with respect to the data storage media, the class identifier, when combined with a user authentication message from a user of the authorized class of users in accordance with the predetermined algorithm, authorizes the user (see Schneck et al., column 23, line 56 through column 24, line 4); and wherein the computer processor additionally, upon receiving the user authentication messages from the data storage drive via the wireless interface (see Davis, column 3, lines 19-24), combining the user authentication message with the class identifier from the class table in accordance with the predetermined algorithm to authorize or deny the class activity to the user (see Schneck et al., column 23, line 56 through column 24, line 4), and transmitting the class authorization or denial to the data storage drive via the wireless interface (see Davis, column 3, lines 19-24).

As to claims 11, 25, 37 and 48, Schneck et al. as modified, teaches wherein the computer processor user table additionally comprises any class membership of each the user, wherein the user may be authorized with respect to the class table either by the class authorization or by the user authorization (see Schneck et al., column 23, line 56 through column 24, line 4).

As to claims 12, 26, and 49, Schneck et al. as modified, teaches wherein the computer processor user table and the class table permitted activities comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table (see Schneck et al., column 22, line 65 through column 23, line 60).

As to claims 13, and 27, Schneck et al. as modified, teaches wherein the computer processor additionally comprises a nonvolatile memory storing the user table and the class table (see Schneck et al., column 14, line 66 through column 15, line 13).

As to claims 14, 28, 39, and 50, Schneck et al. as modified, teaches wherein the data stored in the data storage media is encrypted (see Schneck et al., column 13 lines 1-2), wherein the computer processor user table permitted activities comprise at least 1)

read access to data stored in the data storage media (see Schneck et al., column 23, lines 6-55), and wherein the user authorization for the read access additionally comprises a decryption key for the encrypted stored data (see Schneck et al., column 26, lines 52-57).

As to claim 15, Schneck et al. teaches, the computer processor having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 23, line 56 through column 24, line 4, where the "user table" is read on the permission list that has a list of users or groups of users and there qualities and quantities of access), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user; the user authentication messages from the data storage drive, combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity, and the user authorization or denial to the data storage drive (see column 10, line 59 through column 11, line 3).

Schneck et al. does not teach a data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, comprising: data storage media mounted in the data storage cartridge for storing the data for the read/write access; a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data

storage drive when mounted in the data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface, and transmitting via the wireless interface.

Davis teaches a data storage cartridge for storing data for read/write access (see column 3, lines 24-29) by a user of a data storage drive when mounted in the data storage drive (see column 5, lines 55-61), comprising: data storage media mounted in the data storage cartridge for storing the data for the read/write access (see column 3, lines 24-29); a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive (see column 3, 19-23); and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface (see column 6, lines 22-59); the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface (see column 3, lines 19-23); the computer processor receiving via the wireless interface, and transmitting via the wireless interface (see column 3, lines 19-23).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. to included a data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, comprising: data storage media mounted in the data storage cartridge for storing the data for the read/write access; a wireless interface

mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface, and transmitting via the wireless interface.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. by the teachings of Davis to include a data storage cartridge for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, comprising: data storage media mounted in the data storage cartridge for storing the data for the read/write access; a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive; and a computer processor mounted in the portable data storage cartridge and coupled to the wireless interface; the computer processor powered by the wireless interface and receiving and transmitting data to the data storage drive via the wireless interface; the computer processor receiving via the wireless interface, and transmitting via the wireless interface because this would be one form of a storage device that could tangibly embody a package of digital data comprising protected portions (see Schneck et al., column 7, lines 28-30).

As to claim 29, Schneck et al., teaches having a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 23, line 56 through column 24, line 4, where the "user table" is read on the permission list that has a list of users or groups of users and there qualities and quantities of access), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user, the method comprising the steps of: the user authentication messages from the data storage drive; combining the user authentication message with the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity; and the user authorization or denial to the data storage drive (see column 10, line 59 through column 11, line 3).

Schneck et al. does not teach a method for providing a portable secure interface to a data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, the data storage cartridge the method comprising steps of: receiving via the wireless interface; and transmitting via the wireless interface.

Davis teaches a method for providing a portable secure interface to a data storage cartridge, the data storage cartridge having data storage media for storing data

for read/write access by a user of a data storage drive (see column 3, lines 24-29) when mounted in the data storage drive (see column 5, lines 55-61), and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, the data storage cartridge the method comprising steps of: receiving via the wireless interface; and transmitting via the wireless interface (see column 3, lines 19-23).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. to include a method for providing a portable secure interface to a data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, the data storage cartridge the method comprising steps of: receiving via the wireless interface; and transmitting via the wireless interface.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. by the teachings of Davis because a method for providing a portable secure interface to a data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data

storage drive, the data storage cartridge the method comprising steps of: receiving via the wireless interface; and transmitting via the wireless interface would be one form of a storage device that could tangibly embody a package of digital data comprising protected portions (see Schneck et al., column 7, lines 28-30).

As to claims 32 and 43, Schneck et al. as modified, teaches wherein the user authentication message is encrypted by a sender private key and a receiver public key, wherein the public key cryptographic algorithm decrypts the user authentication message employing a receiver private key and the sender public key, and wherein the combining step comprises decrypting the user authentication message by the receiver private key and the sender public key, whereby the user authentication message is known to have come from the user (see Schneck et al., column 10, line 59 through column 11, line 3).

As to claim 33, Schneck et al. as modified, teaches wherein the user table comprises a plurality of the permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read the user entry of the user table, 4) read all entries of the user table, 5) add entries to the user table, and 6) change/delete entries to the user table; and wherein the transmitting step comprises transmitting authorization to conduct the

selected the user permitted activities the user is authorized to conduct (see Schneck et al., column 23, lines 6-55 and see column 32, lines 15-27).

As to claim 34, Schneck et al. as modified, teaches wherein the user table comprises a separate entry for each the user identifier and the permitted activity the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted activities from the separate entries (see Schneck et al., column 23, lines 6-55 and see column 32, lines 15-27).

As to claim 35, Schneck et al. as modified, teaches wherein the step of providing the user table comprises a separate entry for each the user identifier, the entry comprising all the permitted activities the user is authorized to conduct; and wherein the transmitting step additionally comprises identifying the user permitted 20 activities from the user separate entry (see Schneck et al., column 23, lines 6-55 and see column 32, lines 15-27).

As to claim 38, Schneck et al. as modified, teaches wherein the user table and the class table comprise a plurality of permitted activities, selected ones of which each of the users may be authorized to conduct, the permitted activities comprising 1) read access to data stored in the data storage media, 2) write access to data stored in the data storage media, 3) read all entries of the class table, 4) add entries to the class table, and 5) change/delete entries to the class table; and wherein the transmitting step

comprises transmitting authorization to conduct the selected the user and the class permitted activities the user is authorized to conduct (see Schneck et al., column 23, lines 6-55 and see column 32, lines 15-27).

As to claim 40, Schneck et al., teaches a computer program product usable with a programmable computer processor having computer readable program code (see column 18, lines 3-6) embodied therein for providing a secure interface (see Abstract), the computer program product comprising:

computer readable program code which causes the programmable computer processor to provide a user table comprising at least a unique user identifier for each authorized user and at least one permitted activity the user is authorized to conduct with respect to the data storage media (see column 23, line 56 through column 24, line 4, where the "user table" is read on the permission list that has a list of users or groups of users and there qualities and the quantities of access), the user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user (see column 10, line 59 through column 11, line 3);

computer readable program code which causes the programmable computer processor (see column 18, lines 3-6) to receive the user authentication messages from the data storage drive (see column 10, line 59 through column 11, line 3);

computer readable program code which causes the programmable computer processor (see column 18, lines 3-6) to combine the user authentication message with

the user identifier from the user table in accordance with the predetermined algorithm to authorize or deny the user activity (see column 10, line 59 through column 11, line 3); and

computer readable program code which causes the programmable computer processor (see column 18, lines 3-6) to transmit the user authorization or denial to the data storage drive via the wireless interface (see column 10, line 59 through column 11, line 3).

Schneck et al. does not teach to a data storage cartridge, the programmable computer processor mounted in the data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, receive via the wireless interface, and transmit via the wireless interface.

Davis teaches to a data storage cartridge (see column 2, line 45), the programmable computer processor mounted in the data storage cartridge (see column 6, lines 22-59), the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive (see column 3, lines 24-29) when mounted in the data storage drive (see column 5, lines 55-61, where "mounted in the data storage drive" is read on "brought into proximity"), and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive (see

column 3, lines 19-23), receive via the wireless interface, and transmit via the wireless interface (see column 3, lines 19-23).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schneck et al. to include to a data storage cartridge, the programmable computer processor mounted in the data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, receive via the wireless interface, and transmit via the wireless interface.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Schenck et al. by the teachings of Davis because to a data storage cartridge, the programmable computer processor mounted in the data storage cartridge, the data storage cartridge having data storage media for storing data for read/write access by a user of a data storage drive when mounted in the data storage drive, and a wireless interface mounted in the portable data storage cartridge for receiving power and data from, and sending data to, the data storage drive when mounted in the data storage drive, receive via the wireless interface, and transmit via the wireless interface would this would be one form of a storage device that could tangibly embody a package of digital data comprsing protected portions (see Schneck et al., column 7, lines 28-30).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of art with respect to portable data access in general.

U.S. patent No. 5,889,866 issued to Cyras et al. for teaching controlling access to detachably connectable computer devices.

U.S. patent No. 5,982,520 issued to Weiser et al. for teaching a personal storage device for application and data transfer.

U.S. patent No. 6,092,201 issued to Turnbull et al. for teaching secured communication operations via a shared list.

U.S. patent No. 6,446,206 B1 issued to Feldbaum for teaching user authentication.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

jfb
October 14, 2003

DOV POPOVICI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100